R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR 00/02009

REC'D 26 SEP 2000
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

4

FR 00/02009

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 18 AOUT 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITE

PRESENTE OU TRANSMIS CONFORMEMENT A LA REGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

26bis, rue de Saint-Pétersbourg
75800 Paris Cedex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livreVI

REQUÊTE EN DÉLIVRANCE

0	**RESERVE A L'INPI**	
0-1	**Date de remise des pièces**	15.07.99
0-2	**N° d'enregistrement national**	9909316
0-3	**Département de dépôt**	99
0-4	**Date de dépôt**	15 JUIL. 1999

0-6	**Titre de l'invention**	Procédé d'amélioration d'un générateur aléatoire en vue de le rendre résist contre les attaques par mesure de courant
0-8	**Etablissement du Rapport de Recherche**	immédiat
0-9	**Votre référence dossier**	GEM736
1	**DEMANDEUR(s)**	
1-1	*Nom*	GEMPLUS
	Suivi par	BRUYERE Pierre
	Adresse rue	Avenue du Pic de Bertagne Parc d'activités de Gèmenos
	Adresse code postal et ville	13881, GEMENOS
	Pays	France
	Nationalité	France
	Forme juridique	S.C.A
	N° SIREN	349 711 200
	Code APE-NAF	321B
	N° de téléphone	04.42.36.69.06.
	N° de télécopie	04.42.36.63.43.
	Courrier électronique	nathalie.herail@gemplus.com

4	**Déclaration de PRIORITE ou REQUETE du bénéfice de la date de dépôt d'une demande antérieure**	Etat	Date	N° de la demande
6	**Documents et Fichiers joints**	Fichier électronique	Pages	Détails
6-1	*Description*	easy736.doc	7	
6-2	*Revendications*	easy736.doc	3	8
6-3	*Abrégé*	easy736.doc	1	
6-4	*Listage de séquences*			
6-5	*Rapport de recherche*			
7	**Mode de paiement**	Prélèvement du compte courant		
7-1	*Numéro du compte client*	2381		
7-2	*Remboursement à effectuer sur le compte n°*	2381		

8	**REDEVANCES**	Devise	Taux	Montant à payer
	062 Dépôt	FRF	250.00	
	063 Rapport de recherche (R.R.)	FRF	4 200.00	4
	Total à acquitter	FRF		4

10	Signature	
10-1	*Signé par*	NONNENMACHER Bernard Directeur de la Propriété Industrielle GEMPLUS

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulai
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

Désignation de l'inventeur

Référence utilisateur:	GEM736
Référence système:	111111 729774,640653704
N° d'enregistrement national:	990 916
Titre de l'invention:	Procédé d'amélioration d'un générateur aléatoire vue de le rendre résistant contre les attaques pa mesure de courant
Le(s) soussigné(s):	NONNENMACHER Bernard Directeur de la Propriété Industrielle GEMPLUS
Désigne(nt) en tant qu'inventeur(s):	
Inventeur 1	
Nom, Prénom:	CORON, Jean-Sébastien
Adresse:	4 rue Léon de Lagrange F-75015 PARIS France
Inventeur 2	
Nom, Prénom:	NACCACHE, David
Adresse:	7 rue Chaptal F-75009 PARIS France
Signé par:	NONNENMACHER Bernard Directeur de la Propriété Industrielle GEMPLUS
En qualité de:	Directeur de la Propriété Industrielle
Date:	12 juil. 1999

DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
8 à 10			RM	22/03/2000	30 MARS 2000 - G Y

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

PROCEDE D'AMELIORATION D'UN GENERATEUR ALEATOIRE EN VUE DE LE RENDRE RESISTANT CONTRE LES ATTAQUES PAR MESURE DE COURANT

L'invention concerne une amélioration d'un procédé de génération de nombres aléatoires ou source aléatoire, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce.

Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable.

La plupart des systèmes de cryptographie à clé publique (dite aussi cryptographie asymétrique) et clé secrète (dite aussi cryptographie symétrique) nécessitent le tirage d'aléas secrets. Il est primordial que de tels aléas, ou nombres, destinés à servir comme clés ultérieurement , soient à priori imprévisibles et ne présentent pas de régularités permettant de les retrouver par des stratégies de recherche exhaustive ou exhaustive améliorée pour laquelle les clés les plus probables sont cherchées en premier lieu.

Il est possible de construire une source aléatoire à partir d'une fonction dont il est

difficile de calculer l'inverse. Soit f une telle fonction. Il est possible de construire une source aléaoire en commençant par sélectionner une variable d'initialisation aléatoire s et en appliquant la fonction f à la suite de valeurs s, s+1, s+2,…La sortie de la source aléatoire est définie comme f(s),f(s+1),f(s+2),…En fonction des propriétés de la fonction f utilisée, il peut être préférable de ne garder que quelques bits de la sortie f(s),f(s+1),f(s+2)…

Une méthode de génération de nombre aléatoire à partir d'une fonction dont il est difficile de calculer l'inverse est spécifiée dans le standard ANSI X9.17. La méthode utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Le procédé de génération de nombre aléatoire prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m. Le procédé est caractérisé par les 3 étapes suivantes :

1) Chiffrer avec l'algorithme DES utilisant la clef K une valeur D représentant une information de date et mettre le résultat dans la variable entière I.
2) Pour j allant de 1 à m exécuter les étapes suivantes :
   2)a) Remplacer s par s xor I.

2)b) Mettre dans x_j le résultat du chiffrement de s avec l'algorithme DES utilisant la clef secrète K.

2)c) Remplacer s par x_j xor I.

2)d) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef secrète K.

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

Il est possible d'utiliser ce générateur aléatoire dans une application pour laquelle un générateur aléatoire est déjà disponible, mais de qualité jugée insuffisante, par exemple un générateur aléatoire embarqué dans le microprocesseur d'une carte à puce. Dans ce cas, le procédé décrit précédemment est utilisé pour améliorer la qualité du générateur aléatoire. Ce procédé prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m. Le procédé utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Le procédé utilise une source S de qualité jugée insuffisante d'entiers aléatoires sur 64 bits. Le procédé est caractérisé par les 3 étapes suivantes :

1) Pour j allant de 1 à m faire

1)a) Générer un entier I à l'aide de la source S.

1)b) Remplacer s par s xor I.

1)c) Mettre dans x_j le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

1)d) Générer un entier I à l'aide de la source S.

1)e) Remplacer s par x_j xor I.

1)f) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

2) Retourner en sortie la suite $(x_1, x_2, \ldots, x_m)$.

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé secrète (par exemple l'algorithme DES) était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé secrète. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée. Pour retrouver la clef secrète, il est nécessaire que le message d'entrée ou le message de sortie de l'algorithme de chiffrement soient connus.

Les 2 procédés de génération de nombre aléatoire décrits précédemment sont donc vulnérables à des attaques de type attaques DPA. En effet, les nombres aléatoires renvoyés en sortie par ces 2 procédés sont les messages de sortie de l'algorithme de chiffrement. A partir de la consommation de courant de la carte à

puce, il est donc possible de retrouver la clef K de chiffrement, et donc de prévoir ensuite la sortie du générateur aléatoire.

Le procédé de l'invention consiste en une modification des procédés de générations de nombre aléatoire décrits précédemment de façon à les rendre résistant contre des attaques de type DPA.

Le premier procédé modifié de générations de nombre aléatoire utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Il prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,..., x_m. Le procédé utilise une variable entière intermédiaire y. Le procédé est caractérisé par les trois étapes suivantes :

1) Chiffrer avec l'algorithme DES utilisant la clef k une valeur D représentant une information de date et mettre le résultat dans la variable entière I.
2) Pour j allant de 1 à m exécuter les étapes suivantes :
   2)a) Remplacer s par s xor I.
   2)b) Mettre dans la variable entière y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.
   2)c) Mettre dans x_j le résultat de y xor s.

2)d) Remplacer s par y xor I.

2)e) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

Dans ce procédé amélioré de génération de nombres aléatoires, une attaque par mesure de courant de type DPA est impossible car les messages d'entrée et de sortie de l'algorithme de chiffrement DES ne sont pas connus.

Le second procédé amélioré de génération de nombre aléatoire est utilisé pour augmenter la qualité d'un générateur aléatoire dont la qualité est jugée insuffisante. Ce procédé prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m. Le procédé utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Le procédé utilise une source S de qualité jugée insuffisante d'entiers aléatoires sur 64 bits. Le procédé est caractérisé par les deux étapes suivantes :

1) Pour j allant de 1 à m faire

1)a) Générer un entier I à l'aide de la source S.

1)b) Remplacer s par s xor I.

1)c) Mettre dans y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

1)d) Mettre dans x_i le résultat de y xor s.

1)e) Remplacer s par y xor I.

1)f) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

Dans ce procédé amélioré de génération de nombres aléatoires, une attaque par mesure de courant de type DPA est impossible car les messages d'entrée et de sortie de l'algorithme de chiffrement DES ne sont pas connus.

Les deux procédés de génération de nombre aléatoires précédemment décrits permettent donc d'obtenir un générateur de nombre aléatoire résistant contre les attaques par mesure de courant de type DPA.

FEUILLE AVANT RECTIFICATION

REVENDICATIONS

1- Procédé de génération de nombre aléatoire utilisant l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, ladite clef K ne devant être utilisée que dans le cadre de cet algorithme, ledit procédé prenant en entrée un entier aléatoire et secret s de taille 64 bits et un paramètre entier m, ledit procédé renvoyant en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m, caractérisé en ce qu'il comprend trois étapes :

1) Chiffrer avec l'algorithme DES utilisant la clef K une valeur D représentant une information de date et mettre le résultat dans une variable entière I;

2) Pour j allant de 1 à m faire:

2)a) Remplacer s par s xor I;

2)b) Mettre dans la variable entière y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K;

2)c) Mettre dans x_j le résultat de y xor s;

2)d) Remplacer s par y xor I;

2)e) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef k;

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

2- Procédé de génération de nombre aléatoire permettant d'améliorer la qualité d'un générateur aléatoire dont la qualité est jugée insuffisante, ledit procédé prenant en entrée un entier aléatoire et secret s de taille 64 bits

et un entier m, ledit procédé renvoyant en sortie m entiers aléatoires de taille 64 bits x_1, x_2,…, x_m, ledit procédé utilisant l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme, ledit procédé utilisant une variable intermédiaire entière y, ledit procédé utilisant une source S de qualité jugée insuffisante d'entiers aléatoires sur 64 bits x_1, x_2,…, x_m,, caractérisé en ce qu'il comprend les deux étapes suivantes :

1) Pour j allant de 1 à m faire

1)a) Générer un entier I à l'aide de la source S;

1)b) Remplacer s par s xor I;

1)c) Mettre dans y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef k.

1)d) Mettre dans x_i le résultat de y xor s;

1)e) Remplacer s par y xor I;

1)f) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K;

2) Retourner en sortie la suite (x_1, x_2,…, x_m).

3. Dispositif électronique selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif effectuant le test est un dispositif portable.

4. Dispositif électronique selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif est une carte à puce.

5. Dispositif électronique selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif est une carte sans contact.

6. Dispositif électronique selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif est une carte PCMCIA.

7. Dispositif électronique selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif est un badge.

8. Dispositif électronique selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif est une montre intelligente.

REVENDICATIONS

1- Procédé de génération de nombre aléatoire utilisant l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, ladite clef K ne devant être utilisée que dans le cadre de cet algorithme, ledit procédé prenant en entrée un entier aléatoire et secret s de taille 64 bits et un paramètre entier m, ledit procédé renvoyant en sortie m entiers aléatoires de 64 bits x_1, x_2,..., x_m, caractérisé en ce qu'il comprend trois étapes :

1) Chiffrer avec l'algorithme DES utilisant la clef K une valeur D représentant une information de date et mettre le résultat dans une variable entière I;

2) Pour j allant de 1 à m faire:

2)a) Remplacer s par s xor I;

2)b) Mettre dans la variable entière y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K;

2)c) Mettre dans x_j le résultat de y xor s;

2)d) Remplacer s par y xor I;

2)e) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef k;

3) Retourner en sortie la suite (x_1, x_2,..., x_m).

2- Procédé de génération de nombre aléatoire permettant d'améliorer la qualité d'un

générateur aléatoire dont la qualité est jugée insuffisante, ledit procédé prenant en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, ledit procédé renvoyant en sortie m entiers aléatoires de taille 64 bits x_1, x_2,..., x_m,, ledit procédé utilisant l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme, ledit procédé utilisant une variable intermédiaire entière y, ledit procédé utilisant une source S de qualité jugée insuffisante d'entiers aléatoires sur 64 bits x_1, x_2,..., x_m,, caractérisé en ce qu'il comprend les deux étapes suivantes :

1) Pour j allant de 1 à m faire

1)a) Générer un entier I à l'aide de la source S;

1)b) Remplacer s par s xor I;

1)c) Mettre dans y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef k.

1)d) Mettre dans x_i le résultat de y xor s;

1)e) Remplacer s par y xor I;

1)f) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K;

2) Retourner en sortie la suite (x_1, x_2,..., x_m).

3. Dispositif électronique mettant en œuvre le procédé selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif est un dispositif portable.

4. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte à puce.

5. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte sans contact.

6. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte PCMCIA.

7. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est un badge.

8. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une montre intelligente.